

## Web Application Security

**Student number:** AB0168

**Name:** Mays AL-Azzawi

**Group:** TIC21S

**Time management:** Approximately 10 hours

### Week 04

#### Insecure Design:

##### *JuiceShop – Easter Egg*

**Title:** Find Easter Egg from Juice Shop.

**Description:** Web Application has a file to give instruction about the site and it is work as a robot inside the site and sometimes this file can include a sensitive information or stored password.

#### Steps to produce:

1. Navigate to `https://wasdat.fi/3000`.
2. Login in to the website.
3. Navigate to `https://wasdat.fi/3000/robots.txt`.
4. The robots.txt file include information allowed to navigate to another page  
user-agent:\* ;means applies to all robots  
Disallow: /ftp ; first place to look as it is disallowed
5. In the website : wasdat.fi:3000/ftp. Found an easter.gg file but it is open only as .md file or pdf .  
So navigate to file and add %2500.md
6. The URL : wasdat.fi:3000/ftp/easter.gg%2500.md print a text file which included a further information and got the score.

Kali-Ethical-Hacking-2023-ab0168-6987.vmx - VMware Remote Console

VMRC

File Edit Search View Document Help

```

1["Congratulations, you found the easter egg!"
2 - The incredibly funny developers
3
4 ...
5
6 ...
7
8 ...
9
10 Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real easter egg can be found here:
11
12 L2dici9xcmLmL25lci9mYi9zaGFhbc9ndXJsL3V2c59uY59ybmcUvcnR0L2p2Z3V2YS9ndXVcm5mZ3JlL3J0dA==
13
14 Good luck, egg hunter!

```

Christmas Special	★★★★	Order the Christmas special offer of 2014.	Injection		unsolved
Deprecated Interface	★★	Use a deprecated B2B interface that was not properly shut down.	Security Misconfiguration	Contraption Prerequisite	unsolved
Easter Egg	★★★★	Find the hidden <b>easter egg</b> .	Broken Access Control	Contraption Good for Demos Shenanigans	solved
Empty User Registration	★★	Register a user with an empty email and password.	Improper Input Validation		unsolved
Ephemeral Accountant	★★★★	Log in with the (non-existing) accountant <i>acc0unt4nt@juice-sh.op</i> without ever registering that user.	Injection		unsolved
Expired Coupon	★★★★	Successfully redeem an expired campaign coupon code.	Improper Input Validation		unsolved
Five-Star Feedback	★★	Get rid of all 5-star customer feedback.	Broken Access Control		unsolved
Forgotten Developer Backup	★★★★	Access a developer's forgotten backup file.	Sensitive Data Exposure	Contraption Good for Demos Prerequisite	unsolved
Forgotten Sales Backup	★★★★	Access a salesman's forgotten backup file.	Sensitive Data Exposure	Contraption	unsolved
GDPR Data Theft	★★★★	Steal someone else's personal data without using Injection.	Sensitive Data Exposure		unsolved
Leaked Unsafe Product	★★★★	Identify an unsafe product that was removed from the shop and <b>inform the shop</b> which ingredients are dangerous.	Sensitive Data Exposure	OSINT Shenanigans	unsolved
	★★★★	Inform the <b>shop</b> about a <b>typosquatting</b> trick it has been a victim of at <b>juice-shop</b> .			unsolved

- Impact estimation:
  - Low Severity: User/robot can identify restricted or confidential information on the site and disallow list can serve as a map to the first place to look.
- Mitigation:
  - Ensure it is correctly configuring, understand the purpose of using robots.txt with your site, create user-agent and test the configuration.

*Main target – Coupon codes stored in plain text.*

**Title:** Find and locate a sensitive information containing upcoming coupon codes.

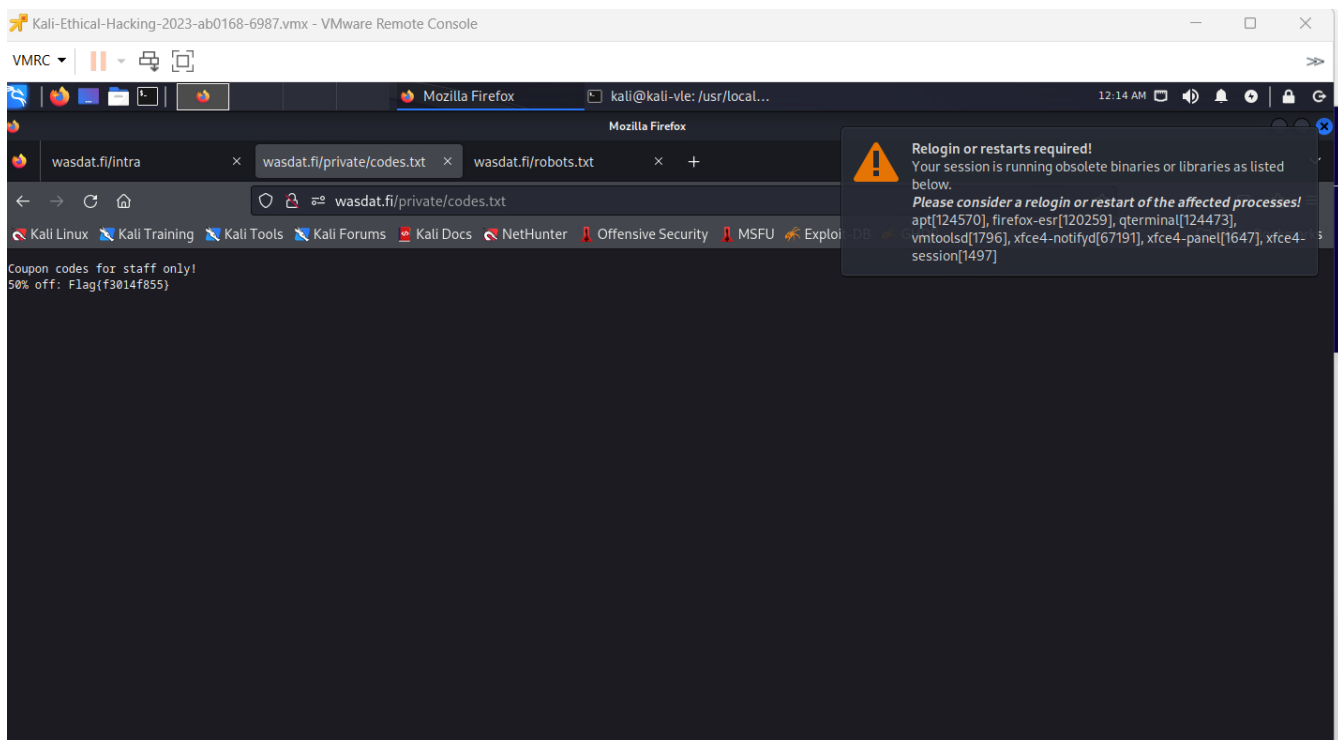
**Description:** Web Application has a robots.txt file which could include or navigate to sensitive information about the site.

**Steps to produce:**

1. Navigate to `https://wasdat.fi`.
2. Navigate to the Robots.txt of the website.  
`http://Wasdat.fi/robots.txt`
3. Inside the robots.txt file there are many disallowed links which need to look and check.
4. When viewing the URLs found `wasdat.fi/private` includes two links.
5. Visit the link for `codes.txt` which may include some information about the code, the text file included the coupon flag.

Coupon codes for staff only!

50% off: Flag{f3014f855}



- Impact estimation:
  - High Severity: User/robot can identify restricted or confidential information on the site and disallow list can serve as a map to the first place to look.
- Mitigation:

- Ensure it is correctly configuring, understand the purpose of using robots.txt with your site, create user-agent and test the configuration.
- 

### *Main target-Login intra :*

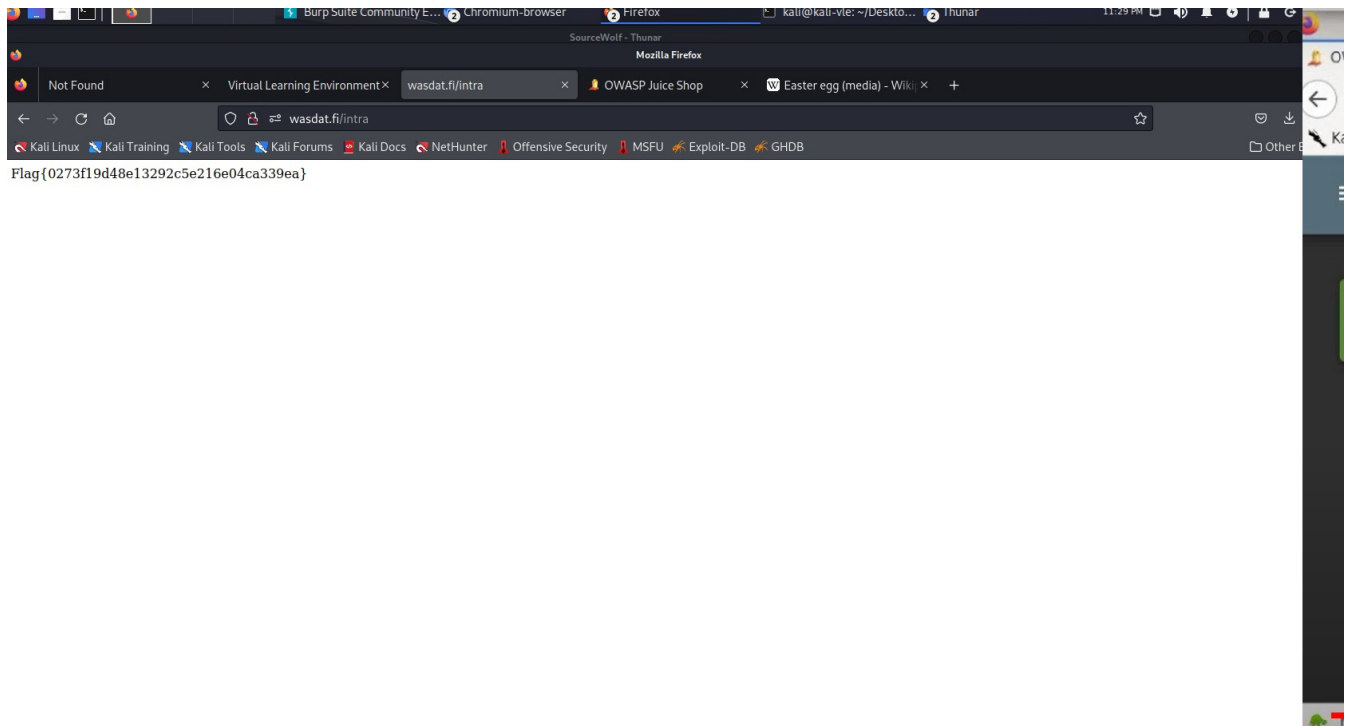
**Title:** find and locate intra with a password stored on the target.

**Description:** In this task we try to digging deeply for further information we can get from the robots.txt to find a credential information like password to login to intra page.

### **Steps to produce:**

1. Navigate to <https://wasdat.fi>.
2. Navigate to the Robots.txt of the website.  
<http://Wasdat.fi/robots.txt>
3. Inside the robots.txt file there are many disallowed linked which need to visit and check.
4. When viewing the URLs found  
[wasdat.fi/intra](http://wasdat.fi/intra): is the intra login page  
[wasdat.fi/private](http://wasdat.fi/private) : includes two links one of them may have a hidden password in a txt.
5. When clicked on [intra-password.conf](http://intra-password.conf) which may include some credential information as the name describes, the file shows an Error and the page only allowed for .txt files.
6. To open a hidden txt files in the page we add %2500.txt so,  
[Wasdat.fi/intra-password.conf%2500.txt](http://Wasdat.fi/intra-password.conf%2500.txt).
7. The txt file includes (IntRa-P@sSW0rd-xyz) a sensitive information which we can use later to login to intra page as a password
8. IntRa-P@sSW0rd-xyz used as a password to login to [wasdat.fi/intra](http://wasdat.fi/intra) and the show a flag which navigate to finish our task.

Flag{0273f19d48e13292c5e216e04ca339ea}



- Impact estimation:
  - high Severity:Users enable to find a sensitive information about the credential of the page.
- Mitigation:
  - Understand the use of robots.txt and review the information and the configuration of the website.